

A Note on Hamming distance of constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}^*$

Hongwei Liu¹, Maouche Youcef^{1,2}

¹School of Mathematics and Statistics, Central China Normal University, Wuhan, Hubei, 430079, China

²Department of Mathematics, University of Sciences and Technology HOUARI BOUMEDIENE, Alger, Algeria

Abstract. For any prime p , λ -constacyclic codes of length p^s over $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ are precisely the ideals of the local ring $\mathcal{R}_\lambda = \frac{\mathcal{R}[x]}{(x^{p^s} - \lambda)}$, where $u^2 = 0$. In this paper, we first investigate the Hamming distances of cyclic codes of length p^s over \mathcal{R} . The minimum Hamming distances of all cyclic codes of length p^s over \mathcal{R} are determined. Moreover, an isometry between cyclic and α -constacyclic codes of length p^s over \mathcal{R} is established, where α is nonzero elements of \mathbb{F}_{p^m} , which carries over the results regarding cyclic codes corresponding to α -constacyclic codes of length p^s over \mathcal{R} .

Keywords. Constacyclic codes; Hamming distances; Repeated-root codes; Codes over rings.

2010 *Mathematics Subject Classification.* Primary 94B15, 94B05; Secondary 11T71.

1 Introduction

Constacyclic codes over finite fields are generalizations of cyclic and negacyclic codes, and it's form a well-known family of linear codes, which form an important class of linear codes containing many optimal codes. However, most of the research is concentrated on the situation when the code length n is relatively prime to the characteristic of the field F . The case where the code length n is not relatively prime to the characteristic of F yields the so-called repeated-root codes. which were first studied by Berman [3], and then by several authors, such as Massey et al. [15], Falkner et al. [11], and Roth and Seroussi [20]. Repeated-root codes were investigated in the most generality in the 1990s by Castagnoli et al. [5], and van Lint [22], where they showed that repeated-root cyclic codes have a concatenated construction, and are asymptotically bad. Nevertheless, such codes are optimal in a few cases, that motivates researchers

*E-Mail addresses: hwliu@mail.ccnu.edu.cn (H. Liu), m.youcef@mails.ccnu.edu.cn (M. Youcef).

to further study this class of codes (see, for example, [21], [17], [23]).

After the realization [4], [12], [16], that many seemingly nonlinear binary codes are actually closely related to linear codes over the ring \mathbb{Z}_4 , codes over \mathbb{Z}_4 in particular, and codes over finite rings in general, have received a great deal of attention. The ring $\mathbb{F}_2 + u\mathbb{F}_2$, where $u^2 = 0$, is interesting because it additively similarly to \mathbb{F}_4 , and multiplicatively similarly to \mathbb{Z}_4 . $(1 - u)$ -constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$ of odd length were first introduced by Qian et al in [19], where it proved that the Gray image of a linear $(1 - u)$ -constacyclic code over $\mathbb{F}_2 + u\mathbb{F}_2$ of odd length is a binary distance invariant linear cyclic code. Later, in [2], Amarra and Nemenzo extended the results to codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$, and studied $(1 - u)$ -constacyclic codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ of length n under the condition $\gcd(n, p) = 1$.

In 2009, Dinh [8] studied the algebraic structure of repeated-root $(\alpha + u\beta)$ -constacyclic codes over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ of length 2^s , and determined the Hamming distances of all such codes under the condition $\beta \neq 0$. In recent years, Dinh extended the results of [8] to codes over $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, and obtained the number of codewords in each of those cyclic codes (see [9]) under the same condition $\beta \neq 0$. If $\beta = 0$ Dinh showed that, unlike the chain ring $\mathcal{R}_{\alpha+u\beta}$, the ring \mathcal{R}_α is a local ring with maximal ideal $\langle 2, x - \alpha_0 \rangle$ but not a chain ring, hence, the structure of the rings \mathcal{R}_α are more complicated, it follows that the Hamming distance is more difficult to compute than that of the chain rings $\mathcal{R}_{\alpha+u\beta}$ case.

In this paper, we continue to study Hamming distance of α -repeated-root constacyclic codes over the rings $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ under the rest condition ($\beta = 0$), where the codes are exactly the ideals of the local ring \mathcal{R}_α , which is a local ring with maximal ideal $\langle 2, x - \alpha_0 \rangle$, but not a chain ring. After giving some preliminaries in Section 2, the rest of the paper is organized as follows. In Section 3, we proceed by first giving the structure and Hamming distances of all constacyclic codes of length p^s over the finite field \mathbb{F}_{p^m} , then we give the structure of α -constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ obtained in [9]. Section 4 addresses the cyclic codes of length p^s over \mathcal{R} , we establish the Hamming distances of cyclic codes over \mathcal{R} . In Section 5, we construct a one-to-one rings isomorphism between \mathcal{R}_1 and \mathcal{R}_α which allows us to apply our results about cyclic codes to α -constacyclic codes over \mathcal{R} .

2 Preliminaries

Let R be a finite commutative ring. An ideal I of R is called principal if it is generated by one element. R is called a principal ideal ring if all the ideals of R are principal. The ring R is called a local ring if R has a unique maximal ideal. Furthermore, R is said to be a chain ring if it is a local principal ideal ring. The following result is well known (cf. [10], Proposition 2.1).

Proposition 2.1. *Let R be a finite commutative ring, then the following conditions are equivalent:*

- (i) *R is a local ring and the maximal ideal M of R is principal, i.e., $M = \langle \gamma \rangle$ for some $\gamma \in R$,*
- (ii) *R is a local principal ideal ring,*
- (iii) *R is a chain ring whose ideals are $\langle \gamma^i \rangle$, $0 \leq i \leq e$, where e is the nilpotency index of γ .*

Moreover, if R is a finite commutative chain ring with maximal ideal $\langle \gamma \rangle$, and the nilpotency index of $\langle \gamma \rangle$ is e , then the cardinality of the ideal $\langle \gamma^i \rangle$ is $|R/\langle \gamma \rangle|^{e-i}$, where $i = 0, 1, \dots, e-1$.

Let R be a finite ring, a code C of length n over R is a nonempty subset of R^n , and the ring R is referred to as the alphabet of the code. If this subset is, in addition, a R -submodule of R^n , then C is called *linear*. For a unit λ of R , the λ -constacyclic (λ -twisted) shift τ_λ on R^n is the shift

$$\tau_\lambda((x_0, x_1, \dots, x_{n-1})) = (\lambda x_{n-1}, x_0, x_1, \dots, x_{n-2}),$$

and a code C is said to be λ -constacyclic if $\tau_\lambda(C) = C$, i.e., if C is closed under the λ -constacyclic shift τ_λ . In case $\lambda = 1$, those λ -constacyclic codes are called cyclic codes, and when $\lambda = -1$, such λ -constacyclic codes are called negacyclic codes.

Each codeword $c = (c_0, c_1, \dots, c_{n-1}) \in C$ is customarily identified with its polynomial representation $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$, and the code C is in turn identified with the set of all polynomial representations of its codewords. Then in the ring $\frac{R[x]}{\langle x^n - \lambda \rangle}$, $xc(x)$ corresponds to a λ -constacyclic shift of $c(x)$. From that, the following fact is well known (cf. [13, 14]) and straightforward:

Proposition 2.2. *A linear code C of length n is λ -constacyclic over R if and only if C is an ideal of $\frac{R[x]}{\langle x^n - \lambda \rangle}$.*

Given n -tuples $x = (x_0, x_1, \dots, x_{n-1}), y = (y_0, y_1, \dots, y_{n-1}) \in R^n$, their inner product or dot product is defined as usual

$$x \cdot y = x_0y_0 + x_1y_1 + \dots + x_{n-1}y_{n-1},$$

evaluated in R . Two n -tuples x, y are called *orthogonal* if $x \cdot y = 0$. For a linear code C over R , its *dual code* C^\perp is the set of n -tuples over R that are orthogonal to all codewords of C , i.e.,

$$C^\perp = \{x \mid x \cdot y = 0, \forall y \in C\}.$$

A code C is called *self-orthogonal* if $C \subseteq C^\perp$, and it is called *self-dual* if $C = C^\perp$. The following result is well known (cf. [6, 13, 14, 18]).

Proposition 2.3. *Let p be a prime and R be a finite chain ring of size p^α . The number of codewords in any linear code C of length n over R is p^k , for some integer $k \in \{0, 1, \dots, \alpha n\}$. Moreover, the dual code C^\perp has p^l codewords, where $k + l = \alpha n$, i.e., $|C| \cdot |C^\perp| = |R|^n$.*

In general, we have the following implication of the dual of a λ -constacyclic code.

Proposition 2.4. *The dual of a λ -constacyclic code is a λ^{-1} -constacyclic code.*

For a word $x = (x_0, x_1, \dots, x_{n-1}) \in R^n$, the Hamming weight of x , denoted by $wt(x)$, is the number of nonzero components of x . The Hamming distance $d(x, y)$ of two words x and y equals the number of components in which they differ, which is the Hamming weight $wt(x - y)$ of $x - y$. For a nonzero linear code C , the minimum Hamming weight $wt(C)$ and the minimum Hamming distance $d(C)$ are the same and defined as the smallest Hamming weight of nonzero codewords of C :

$$d(C) = \min \{wt(x) \mid 0 \neq x \in C\}.$$

The zero code is conventionally said to have Hamming distance 0.

In this paper, we consider all constacyclic codes of length p^s with alphabet $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, consists of all p^m -ary polynomials of degree 0 and 1 in an indeterminate u , and it is closed under p^m -ary polynomial addition and multiplication modulo u^2 . Thus, $\mathcal{R} = \frac{\mathbb{F}_{p^m}[u]}{\langle u^2 \rangle} = \{a + ub | a, b \in \mathbb{F}_{p^m}\}$ is a local ring with maximal ideal $u\mathbb{F}_{p^m}$. Therefore, by Proposition 2.1, it is a chain ring. The ring \mathcal{R} has precisely $p^m(p^m - 1)$ units, which are of the forms $\alpha + u\beta$ and γ , where α, β , and γ are nonzero elements of the field \mathbb{F}_{p^m} .

3 Cyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

In [7], the algebraic structure and Hamming distances of cyclic codes of length p^s over \mathbb{F}_{p^m} were established and given by the following theorem.

Theorem 3.1.[7] Let C be a cyclic code of length p^s over \mathbb{F}_{p^m} . Then $C = \langle (x-1)^i \rangle \subseteq \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1 \rangle}$, for $i \in \{0, 1, \dots, p^s\}$, and its Hamming distance $d(C)$ is completely determined by

$$d(C) = \begin{cases} 1, & \text{if } i = 0, \\ l + 2, & \text{if } lp^{s-1} + 1 \leq i \leq (l+1)p^{s-1} \text{ where } 0 \leq l \leq p-2, \\ (t+1)p^k, & \text{if } p^s - p^{s-k} + (t-1)p^{s-k-1} + 1 \leq i \leq p^s - p^{s-k} + tp^{s-k-1}, \\ & \text{where } 1 \leq t \leq p-1, \text{ and } 1 \leq k \leq s-1, \\ 0, & \text{if } i = p^s. \end{cases}$$

It is easy to verify that the cyclic codes of length p^s over $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ are precisely the ideals of the residue ring $\mathcal{R}_1 = \frac{\mathcal{R}[x]}{\langle x^{p^s}-1 \rangle}$. The following lemma is easy to verify.

Lemma 3.2. For any positive integer n , $(x-1)^{p^n} = x^{p^n} - 1 \in \mathcal{R}[x]$. Moreover, $x-1$ is nilpotent in \mathcal{R}_1 with nilpotency index p^s .

Lemma 3.3. Let $f(x) \in \mathcal{R}_1$. Then $f(x)$ can be uniquely written as

$$f(x) = \sum_{i=0}^{p^s-1} a_i(x-1)^i = f_1(x) + uf_2(x) = a_{0,0} + \sum_{i=1}^{p^s-1} a_{0,i}(x-1)^i + u \sum_{i=0}^{p^s-1} a_{1,i}(x-1)^i,$$

where $a_i = a_{0,i} + ua_{1,i} \in \mathcal{R}$, $a_{0,i}, a_{1,i} \in \mathbb{F}_{p^m}$ and $f_1(x), f_2(x) \in \mathbb{F}_{p^m}[x]$. Furthermore, $f(x)$ is invertible if and only if $a_{0,0} \neq 0$.

Proof. The representation of $f(x)$ follows from the fact that it can be viewed as a polynomial of degree less than p^s over $\mathcal{R}[x]$. Each coefficient a_i of $f(x)$ is an element of \mathcal{R} , that can be expressed uniquely by $a_{0,i}, a_{1,i} \in \mathbb{F}_{p^m}$ as $a_i = a_{0,i} + ua_{1,i}$. Expressing $f(x)$ in this representation, the last assertion follows from the fact that u and $x-1$ are both nilpotent in \mathcal{R}_1 . \square

Theorem 3.4 [9] The ring \mathcal{R}_1 is a local ring with the maximal ideal $\langle u, x-1 \rangle$, but it is not a chain ring. Cyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, i.e., ideals of the ring \mathcal{R}_1 , are

- Type 1 (trivial ideals): $\langle 0 \rangle, \langle 1 \rangle$.
- Type 2 (principal ideals with nonmonic polynomial generators): $\langle u(x-1)^i \rangle$, where $0 \leq i \leq p^s - 1$.

- Type 3 (principal ideals with monic polynomial generators): $\langle (x-1)^i + u(x-1)^t h(x) \rangle$, where $1 \leq i \leq p^s - 1$, $0 \leq t < i$, and either $h(x)$ is 0 or $h(x)$ is a unit.
- Type 4 (nonprincipal ideals): $\langle (x-1)^i + u(x-1)^t h(x), u(x-1)^\omega \rangle$, where $1 \leq i \leq p^s - 1$, with $h(x)$ as in Type 3, and $\deg(h(x)) \leq \omega - t - 1$.

4 Hamming Distance of Cyclic Codes

As we mentioned in Section 3 the cyclic codes over \mathcal{R} are precisely the ideal of the ring \mathcal{R}_1 . In order to compute the Hamming distances of all cyclic codes over \mathcal{R} , we count the Hamming distance of the ideals of the ring \mathcal{R}_1 (Type 2, 3, 4).

Proposition 4.1 Let $C = \langle u(x-1)^i \rangle \subsetneq \mathcal{R}_1$ be a cyclic code of length p^s over \mathcal{R} for some $0 \leq i \leq p^s - 1$. Then its minimum Hamming distance is completely determined by

$$d(C) = \begin{cases} 1, & \text{if } i = 0, \\ l + 2, & \text{if } lp^{s-1} + 1 \leq i \leq (l+1)p^{s-1}, \text{ where } 0 \leq l \leq p-2, \\ (t+1)p^k, & \text{if } p^s - p^{s-k} + (t-1)p^{s-k-1} + 1 \leq i \leq p^s - p^{s-k} + tp^{s-k-1}, \\ & \text{where } 1 \leq t \leq p-1, \text{ and } 1 \leq k \leq s-1. \end{cases} \quad (1)$$

Proof. For $i = 0$ then $C = \langle u \rangle$, it follows that $d(C) = 1$.

For $i \in \{1, 2, \dots, p-1\}$, we have $\frac{\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}}{\langle u \rangle} \simeq \mathbb{F}_{p^m}$ then the ideals $\langle u(x-1)^i \rangle$ of \mathcal{R}_1 , are exactly the set of the ideals $\langle (x-1)^i \rangle$ of $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1 \rangle}$ multiplied by u . Hence, the Hamming distance of $\langle u(x-1)^i \rangle$ follows from Theorem 3.1. \square

In order to compute the minimum Hamming distances of those codes for the rest cases (Type 3 and 4), we need the following very useful lemma.

Lemma 4.2 Let $c(x) = a(x) + ub(x)$ be a nonzero polynomial in \mathcal{R}_1 , where $a(x), b(x) \in \mathbb{F}_{p^m}[x]$. Then

we have

$$wt(c(x)) \geq \max\{wt(a(x)), wt(b(x))\}.$$

Proof. By Lemma 3.3, $c(x)$ can be written as

$$c(x) = \sum_{i=0}^{p^s-1} (a_i + ub_i)x^i = a(x) + ub(x) = \sum_{i=0}^{p^s-1} a_i x^i + u \sum_{i=0}^{p^s-1} b_i x^i.$$

Now suppose $wt(a(x)) = d$, then there exist exactly d nonzero $a_{i_k} \in \mathbb{F}_{p^m}$, where $k \in \{1, 2, \dots, d\}$. Note that $c_i = a_i + ub_i$ and $c_i = 0$ if and only if $a_i = b_i = 0$. Hence $c_{i_k} \neq 0 \ \forall i \in \{1, 2, \dots, d\}$. Therefore, $wt(c(x)) \geq d = wt(a(x))$. We can show that $wt(c(x)) \geq wt(b(x))$ by using the similar way.

Since $wt(c(x)) \geq wt(a(x))$ and $wt(c(x)) \geq wt(b(x))$, we get $wt(c(x)) \geq \max\{wt(a(x)), wt(b(x))\}$. \square

Proposition 4.3 Let $C = \langle (x-1)^i + u(x-1)^t h(x) \rangle$ be a cyclic code of length p^s over \mathcal{R} for $1 \leq i \leq p-1$. Then the Hamming distance of C is

$$d(C) = \begin{cases} l+2, & \text{if } lp^{s-1} + 1 \leq i \leq (l+1)p^{s-1}, \text{ where } 0 \leq l \leq p-2, \\ (t+1)p^k, & \text{if } p^s - p^{s-k} + (t-1)p^{s-k-1} + 1 \leq i \leq p^s - p^{s-k} + tp^{s-k-1}, \\ & \text{where } 1 \leq t \leq p-1, \text{ and } 1 \leq k \leq s-1. \end{cases} \quad (2)$$

Proof. Let $c(x)$ be an arbitrary nonzero element of C , then $c(x)$ can be written as

$$c(x) = (a(x) + ub(x))((x-1)^i + u(x-1)^t h(x)),$$

where $a(x), b(x) \in \mathbb{F}_{p^m}[x]$. We consider $c(x)$ in two cases.

Case 1: $a(x) \neq 0$. Then we have

$$\begin{aligned} c(x) &= (a(x) + ub(x))((x-1)^i + u(x-1)^t h(x)) \\ &= a(x)(x-1)^i + u(b(x)(x-1)^i + a(x)(x-1)^t h(x)) \\ &= a(x)(x-1)^i + uh'(x) \end{aligned}$$

where $h(x), h'(x) \in \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1 \rangle}$. By Lemma 4.2, we obtain that

$$wt(c(x)) \geq \max\{wt(a(x)(x-1)^i), wt(h'(x))\} \geq wt(a(x)(x-1)^i).$$

Case 2: $a(x) = 0$. In this case, $b(x) \neq 0$. We have $c(x) = ub(x)(x-1)^i$, and it is easy to see that $wt(c(x)) = wt(b(x)(x-1)^i)$.

We have shown that for every nonzero element $c(x)$ in C , there exist an element $d(x)$ in the ideal $\langle (x-1)^i \rangle$ of the ring $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1 \rangle}$, such that $wt(c(x)) \geq wt(d(x))$. Therefore, $d(C) \geq d(\langle (x-1)^i \rangle)$.

On the other hand we have that

$$u(x-1)^i = u((x-1)^i + u(x-1)^t h(x)) \in C$$

then $\langle u(x-1)^i \rangle \subseteq C$. Hence, $d(\langle (x-1)^i \rangle) = d(\langle u(x-1)^i \rangle) \geq d(C)$, and we get $d(C) = d(\langle (x-1)^i \rangle)$. The rest of the proof follows from Theorem 3.1 and the discussion above. \square

Proposition 4.4 Let i and ω be two positive integers such as described in Theorem 3.4 and let

$$C = \langle (x-1)^i + u(x-1)^t h(x), u(x-1)^\omega \rangle.$$

Then the Hamming distance of C is given by

$$d(C) = \begin{cases} l+2, & \text{if } lp^{s-1} + 1 \leq \omega \leq (l+1)p^{s-1}, \text{ where } 0 \leq l \leq p-2, \\ (t+1)p^k, & \text{if } p^s - p^{s-k} + (t-1)p^{s-k-1} + 1 \leq \omega \leq p^s - p^{s-k} + tp^{s-k-1}, \\ & \text{where } 1 \leq t \leq p-1, \text{ and } 1 \leq k \leq s-1. \end{cases} \quad (3)$$

Proof. We can easily see that $\omega < i$, otherwise C is a principal ideal.

Let $c(x)$ be an arbitrary nonzero element of C , then $c(x)$ can be represented as

$$c(x) = (a(x) + ub(x))((x-1)^i + u(x-1)^t h(x)) + u(x-1)^\omega g(x)$$

where $a(x), b(x)$, and $g(x)$ are elements of $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1 \rangle}$. We consider two cases.

Case 1: $a(x) \neq 0$. Then we can write $c(x)$ as

$$\begin{aligned} c(x) &= (a(x) + ub(x))((x-1)^i + u(x-1)^t h(x)) + u(x-1)^\omega g(x) \\ &= a(x)(x-1)^i + u(b(x)(x-1)^i + (x-1)^\omega g(x)) \\ &= a(x)(x-1)^i + uh'(x) \end{aligned}$$

where $h'(x) \in \frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1 \rangle}$, using the Lemma 4.2 it follows that $wt(c(x)) \geq wt(a(x)(x-1)^i) \geq d(\langle (x-1)^i \rangle)$. Because $\langle (x-1)^i \rangle \subsetneq \langle (x-1)^\omega \rangle$ we have $wt(c(x)) \geq d(\langle (x-1)^\omega \rangle)$.

Case 2: $a(x) = 0$ then we can written $c(x)$ as

$$\begin{aligned} c(x) &= u(b(x)(x-1)^i + (x-1)^\omega g(x)) \\ &= u(x-1)^\omega (b(x)(x-1)^{i-\omega} + g(x)) \\ &= u(x-1)^\omega h'(x), \end{aligned}$$

where $h'(x)$ is nonzero polynomial in $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1 \rangle}$, and therefore we have

$$wt(c(x)) \geq wt((x-1)^\omega h'(x)).$$

We have shown that for any nonzero element in C , there exist an element $e(x)$ in the ideal $\langle (x-1)^\omega \rangle$ such that $wt(c(x)) \geq wt(e(x))$. Therefore, $d(C) \geq d(\langle (x-1)^\omega \rangle)$.

On the other hand we have $\langle u(x-1)^\omega \rangle \subsetneq C$, Hence, the proof follows from Theorem 3.1 and the discussion above. \square

Now we can summarize the above results as the following theorem.

Theorem 4.5 The minimum Hamming distances of all cyclic codes of length p^s over \mathcal{R} are given as follows:

- For codes of $\langle 0 \rangle, \langle 1 \rangle$, their minimum Hamming distance are 0, 1 respectively.
- For codes of $\langle u(x-1)^i \rangle$ where $0 \leq i \leq p^s - 1$, their minimum Hamming distance are given in (1).
- For codes of $\langle (x-1)^i + u(x-1)^t h(x) \rangle$, where $1 \leq i \leq p^s - 1$, $0 \leq t < i$, and either $h(x)$ is 0 or $h(x)$ is a unit, their minimum Hamming distance are given in (2).
- For codes of $\langle (x-1)^i + u(x-1)^t h(x), u(x-1)^\omega \rangle$, where $1 \leq i \leq p^s - 1$, with $h(x)$ as in Type 3, and $\deg(h) \leq \omega - t - 1$, their minimum Hamming distance are given in (3).

5 Hamming Distance of Constacyclic Codes

In the last of the paper, we focus on the minimum Hamming distance of constacyclic codes over \mathcal{R} .

Let α be nonzero elements of the field \mathbb{F}_{p^m} , and β be an elements of the field \mathbb{F}_{p^m} , then $\lambda = \alpha + u\beta$ is a unit of \mathcal{R} . Therefore, there are $p^m(p^m - 1)$ constacyclic codes corresponding to the units λ , for $\beta \neq 0$ the Hamming distances of $(\alpha + u\beta)$ -constacyclic codes were studied in [9]. In the reminder of the section, we address the α -constacyclic codes by constructing one-to-one correspondence between cyclic and α -constacyclic codes to apply our results to α -constacyclic codes.

Note that α is a nonzero element of the finite field \mathbb{F}_{p^m} , then we have $\alpha^{p^m} = \alpha$. By the Division Algorithm, there exist nonnegative integers α_q, α_r such that $s = \alpha_q m + \alpha_r$ with $0 \leq \alpha_r \leq m - 1$. Let $\alpha_0 = \alpha^{-p^{(\alpha_q+1)m-s}} = \alpha^{-p^{m-\alpha_r}}$. Then $\alpha_0^{p^s} = \alpha^{-p^{(\alpha_q+1)m}} = \alpha^{-1}$. This observation leads to the following proposition.

Proposition 5.1 Let φ be the map $\varphi : \frac{\mathcal{R}[x]}{\langle x^{p^s}-1 \rangle} \longrightarrow \frac{\mathcal{R}[x]}{\langle x^{p^s}-\alpha \rangle}$, given by $\varphi(f(x)) = f(\alpha_0 x)$, Then φ is a ring isomorphism, and it is Hamming weight preserving.

Proof. Let $f(x), g(x) \in \mathcal{R}[x]$, then

$$f(x) \equiv g(x) \pmod{x^{p^s}-1} \Leftrightarrow f(x) = g(x) + h(x)(x^{p^s}-1),$$

where $h(x) \in \mathcal{R}[x]$, which is equivalent to

$$f(\alpha_0 x) = g(\alpha_0 x) + h(\alpha_0 x)(\alpha_0^{p^s} x^{p^s} - 1) = g(\alpha_0 x) + \alpha^{-1} h(\alpha_0 x)(x^{p^s} - \alpha),$$

which is equivalent also to $f(\alpha_0 x) \equiv g(\alpha_0 x) \pmod{x^{p^s}-\alpha}$. This means that for $f(x), g(x) \in \frac{\mathcal{R}[x]}{\langle x^{p^s}-1 \rangle}$, $\varphi(f(x)) = \varphi(g(x))$ if and only if $f(x) = g(x)$. This implies that φ is well-defined. It is easy to verify that φ is an ring isomorphism and weight-preserving. \square

The above ring isomorphism φ provides a one-to-one correspondence between cyclic and α -constacyclic code of length p^s over \mathcal{R} . Hence we have the following theorem.

Theorem 5.2 Assume the notation give above. Then the minimum Hamming distances of all α -constacyclic codes of length p^s over \mathcal{R} are given as follows.

- For the codes of $\langle 0 \rangle, \langle 1 \rangle$, their minimum Hamming distances are 0, 1 respectively.
- For the codes of $\langle u(\alpha_0 x - 1)^i \rangle$ where $0 \leq i \leq p^s - 1$, their minimum Hamming distances are given in (1).
- For the codes of $\langle (\alpha_0 x - 1)^i + u(\alpha_0 x - 1)^t h(x) \rangle$, where $1 \leq i \leq p^s - 1$, $0 \leq t < i$, and either $h(x)$ is 0 or $h(x)$ is a unit, their minimum Hamming distances are given in (2).
- For the codes of $\langle (\alpha_0 x - 1)^i + u(\alpha_0 x - 1)^t h(x), u(\alpha_0 x - 1)^\omega \rangle$, where $1 \leq i \leq p^s - 1$, with $h(x)$ as in Type 3, and $\deg(h) \leq \omega - t - 1$, their minimum Hamming distances are given in (3).

Remark 5.3 As pointed out in Section 3, α -constacyclic codes of length p^s over \mathcal{R} are ideals of the ring \mathcal{R}_α , which are not chain rings. For the cases $\mathcal{R}_{\alpha+u\beta}$ where $\beta \neq 0$. In [8] Dinh determined the Hamming

distance for $\mathcal{R}_{\alpha+u\beta}$ where $p = 2$. In [9] Dinh extended these results for all prime numbers. The aim of this paper is the determination of the Hamming distance for the rest cases ($\beta = 0$), where \mathcal{R}_α is a local ring, but not a chain ring.

When $p = 2$, Theorem 5.2 and Theorem 5.1 of [8] complement each other in the sense that they deal with λ -constacyclic over \mathcal{R} . Furthermore, for any prime number Theorem 5.2 and Theorem 4.4 of [9] complement each other in the sense that they deal with λ -constacyclic over \mathcal{R} .

References

- [1] T. Abualrub, and O. Robert. On the generators of \mathbb{Z}_4 cyclic codes of length 2^e . IEEE Transactions on Information Theory 49, no. 9 (2003):2126-2133.
- [2] M.C.V. Amarra, and R.N. Fidel . On $(1 - u)$ -cyclic codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$. Applied Mathematics Letters 21, no. 11 (2008): 1129-1133.
- [3] S.D. Berman. Semisimple cyclic and Abelian codes. II. Cybernetics and Systems Analysis 3, no. 3 (1967): 17-23.
- [4] A.R. Calderbank, A.R. Hammons, P. Vijay Kumar, N.J.A. Sloane, and S. Patrick. A linear construction for certain Kerdock and Preparata codes. Bulletin of the American Mathematical Society 29, no. 2 (1993): 218-222.
- [5] G. Castagnoli, J.L. Massey, A.S. Philipp, and V.S. Niklaus. On repeated-root cyclic codes. IEEE Transactions on Information Theory 37, no. 2 (1991): 337-342.
- [6] H.Q. Dinh. Negacyclic codes of length 2^s over Galois rings. IEEE Transactions on Information Theory 51, no. 12 (2005): 4252-4262.
- [7] H.Q. Dinh. On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions. Finite Fields and Their Applications 14, no. 1 (2008): 22-40.
- [8] H.Q. Dinh. Constacyclic codes of length 2^s over galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE Transactions on Information Theory 55, no. 4 (2009): 1730-1740.
- [9] H.Q. Dinh. Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Journal of Algebra 324, no. 5 (2010): 940-950.
- [10] H.Q. Dinh, and R. Sergio, L.Permouth. Cyclic and negacyclic codes over finite chain rings. IEEE Transactions on Information Theory 50, no. 8 (2004): 1728-1744.
- [11] G. Falkner, B. Kowol, W. Heise, and E. Zehendner. On the existence of cyclic optimal codes. Atti Sem. Mat. Fis. Univ. Modena 28 (1979): 326-341.
- [12] A.R Hammons, P.K. Vijay, A.C. Robert, J.S. Neil, and S.Patrick. The \mathbb{Z}_4 -linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Transactions on Information Theory 40, no. 2 (1994): 301-319.

- [13] W.C. Huffman, and V. Pless. Fundamentals of error-correcting codes. Cambridge university press, 2010.
- [14] F.J. MacWilliams, and N.J.A Sloane. The theory of error correcting codes. Elsevier, 1977.
- [15] J.L. Massey, J.C. Daniel, and J.Jorn. Polynomial weights and code constructions. IEEE Transactions on Information Theory 19, no. 1 (1973): 101-110.
- [16] A.A. Nechaev. Kerdock code in a cyclic form. Discrete Mathematics and Applications 1, no. 4 (1991): 365-384.
- [17] C.S. Nedeloaia. Weight distributions of cyclic self-dual codes. IEEE Transactions on Information Theory 49, no. 6 (2003): 1582-1591.
- [18] V. Pless, A. Richard, Brualdi, and C.W Huffman. Handbook of coding theory. Elsevier Science Inc., 1998.
- [19] J.F. Qian, L.N. Zhang, and S.X. Zhu. $(1 + u)$ constacyclic and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$. Applied Mathematics Letters 19, no. 8 (2006): 820-823.
- [20] R. Roth, and S. Gadiel. On cyclic MDS codes of length q over $\text{GF}(q)$ (Corresp.). IEEE transactions on information theory 32, no. 2 (1986): 284-285.
- [21] L. Tang, B.S. Cheong, and G.Erry. A note on the q -ary image of a q^m -ary repeated-root cyclic code. IEEE Transactions on Information Theory 43, no. 2 (1997): 732-737.
- [22] L. Van, H. Jacobus. Repeated-root cyclic codes. IEEE Transactions on Information Theory 37, no. 2 (1991): 343-345.
- [23] K.H. Zimmermann. On generalizations of repeated-root cyclic codes. IEEE Transactions on Information Theory 42, no. 2 (1996): 641-649.